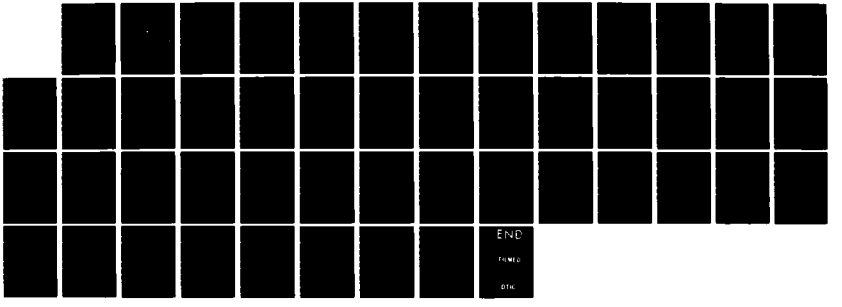
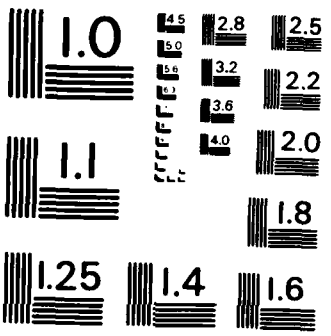
AD-A161 213 EXAMINATION OF RETINAL PATTERN THRESHOLD LEVELS AND THEIR POSSIBLE EFFECT ON COMPUTER ACCESS CONTROL MECHANISMS(U) NAVAL POSTGRADUATE SCHOOL MONTEREY CA 1/1

UNCLASSIFIED D K HELLE SEP 85 F/G 6/2 NL





NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

EXAMINATION OF RETINAL PATTERN THRESHOLD LEVELS AND THEIR POSSIBLE EFFECT ON COMPUTER ACCESS CONTROL MECHANISMS

by

Debra K. Helle

September 1985

Thesis Advisor: Gary K. Poock

Approved for public release; distribution is unlimited

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO. AD-A161213	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Examination of Retinal Pattern Threshold Levels And Their Possible Effect On Computer Access Control Mechanisms		5. TYPE OF REPORT & PERIOD COVERED Master's Thesis September 1985
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Debra K. Helle		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Postgraduate School Monterey, CA 93943-5100		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Naval Postgraduate School Monterey, CA 93943-5100		12. REPORT DATE September 1985
		13. NUMBER OF PAGES 47
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution is unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

access control, computer security, retinal pattern recognitions, authorization techniques, identity verifications

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The advent of multi-programming and the proliferation of shared computer systems has increased the need for greater computer security. Computer security can be segmented into six categories: physical, hardware, software, personnel, communications and procedures. Embedded into software security are those features which protect the system against both unauthorized access and denial of service to authorized users. Another term for this is access control. Access control mechanisms verify (Continued)

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

S/N 0102-LF-014-6601

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

ABSTRACT (Continued)

an individual's identity via three distinct methods: 1) something an individual knows, 2) something an individual possesses or 3) something about the individual. One device which keys on something about the individual is a retinal scan system. This system utilizes the retinal blook vessel pattern as a unique identifier. This thesis studies one such retinal pattern recognition device. For the purposes of this study, an experiment was designed and conducted which determined the reliability of this system as a function of various tolerance levels, as well as its applicability as a computer systems access control mechanism. The Eye Dentify 7.5 system by Eye Dentify Inc., of Portland, Oregon, proved to be a fairly expensive, highly reliable access control device. Its probability for false recognitions is far better than most other known devices. It can be used as a physical access device at virtually any military installation where access devices are used.

Approved for public release; distribution is unlimited.

Examination of Retinal Pattern Threshold Levels And Their Possible Effect On Computer Access Control Mechanisms

by

Debra K. Helle
Lieutenant, United States Navy
B.S., Southern Connecticut State College, 1978

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
September, 1985

Author: Debra K. Helle
Debra K. Helle

Approved by: G.K. Poock
G.K. Poock, Thesis Advisor

J. La Patra
J. La Patra, Second Reader

Willis R. Greer, Chairman,
Department of Administrative Sciences

K.T. Marshall
Kneale T. Marshall,
Dean of Information and Policy Sciences

ABSTRACT

The advent of multi-programming and the proliferation of shared computer systems has increased the need for greater computer security. Computer security can be segmented into six categories: physical, hardware, software, personnel, communications and procedures. Embedded into software security are those features which protect the system against both unauthorized access and denial of service to authorized users. Another term for this is access control. Access control mechanisms verify an individual's identity via three distinct methods: 1) something an individual knows, 2) something an individual possesses or 3) something about the individual. One device which keys on something about the individual is a retinal scan system. This system utilizes the retinal blood vessel pattern as a unique identifier.

This thesis studies one such retinal pattern recognition device. For the purposes of this study, an experiment was designed and conducted which determined the reliability of this system as a function of various tolerance levels, as well as its applicability as a computer systems access control mechanism. The Eye Dentify 7.5 system by Eye Dentify Inc., of Portland, Oregon, proved to be a fairly expensive, highly reliable access control device. Its probability for false recognitions is far better than most other known devices. It can be used as a physical access device at virtually any military installation where access devices are used.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

I. INTRODUCTION

The advent of multiprogramming, database management systems and distributed computer systems has given rise to the belief that data and computers are "shared resources". As more and more systems are utilized by an ever increasing range of the population, the need for security becomes paramount.

The first conference on computer security in 1967 segmented computer security into six categories: physical, hardware, software, personnel, communications and procedures. Physical security provides safeguards for the system itself against such things as fire, flood, and earthquakes. Hardware security protects all items dealing with computer hardware including terminals, disks, tapes, circuitry etc. Software security deals with the protection mechanisms supporting both systems and applications programs. Personnel security ensures that all personnel are properly cleared and trained as to their role in the use of computers. Communications security addresses the issues reguarding the transmission safeguards of the system. Procedures also need to be established in order to administer the safeguards in all these areas.

Embedded into software security are those features which will protect the system against unauthorized access or modification to sensitive information as well as against denial of service to authorized users. Another term for this is access control. Department of Defense (DOD) policy emphasizes access control as the most significant application of computer security (Fauer, 1984).

Access control involves both identifying an individual as an authorized user and verifying his/her identity before

allowing access. Verification of identification can be made using one or more of three distinct methods: 1)something an individual knows, such as passwords; 2) something an individual possesses, such as a badge or card; 3) something about the individual, such as fingerprints.

In recent years, emphasis has been placed on developing an access device which verifies an individual's identity based upon some kind of personal attribute. These devices key on some particular feature that cannot be lost, stolen or duplicated that distinguishes one individual from another. Examples include such systems as those that compare fingerprints, voice patterns and retinal patterns.

Retinal pattern recognition systems utilize the retinal blood vessel pattern as a unique identifier. The orientation/location of the blood vessels in the back of the eye form a pattern which has proven to be substantially different from individual to individual. Systems keying on this personal attribute take the retinal pattern and store it in memory for use as a reference. When an individual requests access, his/her retinal pattern is compared with that in memory. If the two blood vessel patterns match within a certain tolerance, admission is granted. Otherwise access is denied.

The Eye Dentify 7.5 System by Eye Dentify, Inc. is one such device. It is also the basis of this thesis. For the purposes of this study, an experiment was designed and conducted which determined the reliability of this system as a function of various thresholds, as well as its applicability as a computer system access control mechanism.

II. SECURITY BACKGROUND

A. GENERAL HISTORY

First generation computers had no real need for security. Computers at that time were only capable of operating with one user at a time. The programmer himself was the operator. When he wanted to use the computer he went into a room filled with vacuum tubes and circuits, loaded his program into memory and waited for his program to complete. He then took his program and the results and went away. Because only one user program resided in memory at a time and executed until completion, no protection mechanisms were necessary.

Second generation computers saw the separation of operator and programmer and the introduction of the resident monitor. The resident monitor was a system program which automatically transferred control from one user program to another (Peterson, Silberschatz, 1984). Meanwhile, as in the first generation, only one user program resided in memory at a time and executed until completion. The only protection that was necessary was the need to separate the resident monitor from the user program.

Then in 1964 when IBM first marketed its 360 computer, third generation computers were born. Solid state circuitry and memories that could reach and exceed 128K words made it possible for computers to become general purpose machines. One machine could perform both numerical computation and information processing. Third generation technology also included the introduction of independent input/output (I/O) processors that were capable of operating in parallel with the central processor (CPU), hence the beginning of

multiprogramming (Tangney,1980). Computers were now a "shared resource". The demand for computer usage soared.

In the military environment, security was not a new concept. Sensitive information that had previously been stored and processed manually was and is assigned different classifications, depending upon the damage which can occur to national security if such information were disclosed. Classifications can range from top secret and higher, exposure of which can cause grave damage, to confidential material which, if exposed, can cause some damage. At each agency provisions are required which would authorize access to such information only to those individuals with clearance at the proper level and the "need to know" . Many of the applications being considered for implementation in a computer with multiprogramming needed to be processed concurrently and at these multiple classification levels.

In order to satisfy these requirements the operating system had to be able to effectively separate multilevel information and thwart attempts by malicious users to gain access to information for which they did not possess sufficient clearance. Third generation operating systems proved too unreliable to effectively protect information for the simple reason that they were not constructed with security in mind (ibid). This need was first addressed in the fourth generation of computers.

For fourth generation computers and currently in the fifth generation, security is primarily based on the use of formal mathematical models. The model most commonly used is referred to as the Bell and Lapadula Model.

The Bell and Lapadula Model involves two principle rules. The simple security solution specifies that a user at a certain security level can have read access only to objects at the same or lower security level. The *-property (pronounced "star property") principle stipulates that a

user may modify only those objects which are at the same or higher security levels.

The most prominent methodology based on this mathematical model is the security kernal. Through this model, the kernal implements a reference monitor, that is, uses a system component that checks each reference by subject to an object and determines the validity of the access (Landwehr, 1983).

One of the first groups to study computer security in detail was the Defense Science Board's Task Force on Computer Security, organized by the Advanced Research Projects Agency (now the Defense Advanced Research Projects Agency or DARPA). Formed in 1967, they developed recommendations for appropriate computer security safeguards that would protect classified information in multi-access, resource sharing computer systems (Ware, 1979). The task force concluded that

> "a combination of hardware, software, communication, physical, personnel and administrative procedural safeguards is required for comprehensive security and in particular, software safeguards alone are not sufficient" (National Bureau of Standards(NBS), 1979).

The Department of Defense was the first to promulgate computer security policy in 1972 when it issued DOD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems". A follow-up document, DOD 5200.28-M is known as the ADP Security Manual. In it techniques and procedures are outlined for control in the following areas:

1. Physical - safeguards for the system itself and access to it. Types of measures include vaults, locked doors and armed guards. Other physical security issues include safeguards for
   - fire, flood, earthquake

- hardware maintenance
- file backup
- recovery plans
- control of documentation.

2. Personnel - all personnel must be properly cleared and trained for their responsibilities in handling classified information in computers.
3. Communications - addresses the passive monitoring of electromagnetic emanations and the active wire-tapping of information during transmission.
4. Procedural - establishes a system security officer who coordinates the administration of all applicable safeguards.
5. Software - any security and protection mechanisms supported by the operating system or by any application subsystem. Included are five fundamental characteristics:
   - integrity
   - controlled access
   - isolation
   - identification
   - surveillance

More recently the Office of Management and Budget (OMB) established the minimum requirements for a Federal computer security program when it promulgated OMB Circular A-71. These requirements affect all Federal departments and agencies and include the

> "establishment of physical, administrative and technical safeguards required to adequately protect personal, proprietary and other sensitive data not subject to national security regulations"(Epperly, 1980, p.14).

In addition, in 1978, Transmittal Memorandum 1 of OMB Circular A-71 designated to NBS responsibility for

developing computer security standards and guidelines. These have been published through the Federal Information Processing Standards (FIPS) and categorized into the following areas:

- risk analysis
- contingency planning
- security auditing
- network security
- data encryption
- applications program development
- personal identification.

B. ACCESS CONTROL

In general, information in a computer system needs to be protected in three ways (Landwehr, 1981):

1. against unauthorized access to sensitive information
2. against unauthorized modification
3. against denial of service to authorized users.

DOD approaches these issues in the requirements specified in Part II of the DOD Trusted Computer Systems Evaluation Criteria, entitled "Control Objectives for Accountability" (DOD Computer Security Center, 1984). The control objectives specify the following:

1. individuals must provide identification to the system before being allowed interaction with the system
2. this identification must be authenticated by the system
3. actions taken in the system must be traceable to individuals who have been positively identified and whose identity has been authenticated.

DOD has further stated that the most significant computer security threat and therefore the control measures that are most urgently needed are those that prevent

unauthorized access (Fauer, 1984). In other words, the central issue in developing a secure computer system is one of access control.

The best way to ensure proper access control is to establish a positive, unique identification for each person or entity who is to be granted access. This should involve a two-stage process (Hoffman, 1977):

1. identification - the individual presents some form of identity such as "user name"
2. verification or authentication - privately held information is presented to verify the claimed identity.

The unique identifier or "user name" is generally public information and is unlikely to change. There are three ways in which an individual's identity is verified (James, 1973):

1. something known to the individual - he could memorize a password, secret number, or answer a prearranged set of questions.
2. something possessed by the individual - for example, a badge, card or key.
3. something about the individual - this involves some physical personal characteristic such as fingerprints or voice prints.

1. Something an Individual Knows

Passwords are the most commonly used means of controlling access to computer systems. They are the least expensive and require no special hardware. The biggest disadvantage is this information may become known to an unauthorized user who can then use it as readily as an authorized user. Passwords are assigned to the individual in two general ways. In the first way the user is able to generate his own password. The tendency here is to use familiar words such as family name, locations and addresses.

While these are, in most cases, easy to remember, they may also be more easily discovered by a would-be perpetrator. The second method allows the operating system to generate passwords in a highly randomized fashion. While these do not suffer the same threat of exposure of user generated passwords, they are usually very difficult to remember. As a result, the user will not commit it to memory; rather, he will carry the password in written form which could be lost or stolen.

2. Something the Individual Possesses

Another means of verification is through possession of a token such as a key or machine-readable card. A token may be used for providing the claimed identity or the user may enter a claimed identity by means of a keyboard or numerical keypad and then use the token to verify the claimed identity (FIPS Pub 83, 1980). The disadvantage here is that a token may be lost or stolen and a penetrater who succeeds in obtaining a token can use it as readily as an authorized user. Inclusion of some type of password scheme may reduce the risk, but the risk involved with the use of passwords must again be considered.

3. Something About the Individual

The ideal solution would be to develop a machine that would always allow an authorized user access, but would also verify identification via some means that can be neither lost, stolen nor duplicated by an imposter. Because of these inherent drawbacks in both passwords and keys or cards, a great deal of research has focused on the possibility of using some form of personal attribute with which to verify an individual's identity (FIPS Pub 83, 1980). These personal attributes or biometric measurements key on some particular form of interpersonal variation which distinguishes one person from another.

Devices already developed which verify identity based on personal attributes generally operate in the following manner:

1. The user enters his/her claimed identity.
2. The device records a series of measurements on the personal attribute.
3. The measured profile is compared with the reference profile (located either in a central location or on some kind of magnetic strip on a card).
4. The resulting value is compared with a preset toleration threshold which results in a binary decision to accept or reject the individual (or to request more data).

One of the chief limitations in using biometric recognition for verification is the difficulty in performing precise, repeatable measurements on the human body. Because of the curvilinear nature of body surfaces and the plasticity of body tissue, it is difficult to establish accurate reference points as well as good registration for taking measurements or pattern matching (ibid).

There are two types of errors that biometric devices can make:

1. Type I errors : falsely rejecting a correct user. This error rate is calculated by dividing the number of false rejections by the total number of verification attempts by authorized individuals.
2. Type II errors : falsely accepting an individual. The type II error rate is calculated by dividing the number of false acceptances by the number of verification attempts.

Because of the imprecise nature of the attribute being used, some type of tolerance must be built into the device. However, the more tolerance allowed in order to reduce type I errors the higher the probability of type II errors.

Other measures of effectiveness which need to be considered when evaluating a biometric device include the following (FIPS Pub 48, 1977):

1. Susceptibility to Circumvention - refers to the ease with which the device might be circumvented altogether without the need for deceiving the recognition logic.
2. Time to Achieve Recognition - the time for biometric sensing, file retrieval and time for correlation processing to occur. User impatience with even moderate inconveniences imposed can lead to attempts to bypass the system by authorized users.
3. Convenience to the User - refers to ease of accepting recognition as well as ease of learning to actuate the recognition scheme.
4. Cost of the Recognition device - how much does the recognition cost in terms of the cost of the information it is to protect? The system should not cost more than the worth of the information, including the hardware and software designed to create it.
5. Processing Required in the Computer System - how many functions of the biometric device require computer programs, processing capacity and storage in a central facility?
6. Reliability and Maintainability - how well will the device perform over time and how fail-safe is it?

C. TYPES OF BIOMETRIC DEVICES

Several methods of identity verification based on personal attributes have been developed and marketed. A few examples are discussed below.

1. Fingerprints

Verifying identity by manual fingerprint comparisons has been used in forensic work for years. The uniqueness of fingerprints for use as a personal attribute has been well established.

Recently, equipment has been produced which obtains, via a scanning device, an image of the fingerprint without the use of ink and then compares this image, or details extracted from it, with information in a reference file. Comparisons can be made two ways. In the first, a direct comparison is made between the "live" print and the file print. The second method processes the signal image into a digital pattern and matches these bytes with the data stored in memory.

Tests conducted have exhibited a type I error rate of 6.5 percent, a type II error rate of 2.3 percent (Fejfar, 1977). Unfortunately, fingerprints are highly deformable, depending upon the pressure of the hand on the scanning device.

2. Hand Geometry

Hand geometry, or the shape of the hand has shown to exhibit sufficient interpersonal variability to serve as a basis for distinguishing one individual from another with an acceptable degree of accuracy. The Equipment measures such aspects as the length of the fingers from the rounding at the end of the finger to the web between the fingers. Most devices are constructed for use with a magnetic strip card in which the reference profile is imbedded. However, the device can also be connected to a central computer which stores the reference data and does the comparison. The major problems associated with hand geometry revolve around the transluscence of skin width of the hand. In addition,

most devices do not account for the fact that fingernails may be cut or grown to different lengths, thereby changing the geometry of the hand.

3. Signature Dynamics

Research in recent years has concluded that the physical motions which occur during the writing of a signature display variances between individuals with very reasonable type I and type II errors. Signatures frequently become so stylized and are done with little conscious attention to formation as to make them difficult to mimic in terms of the dynamic motions associated with them. Devices using signature dynamics measure time varying force information such as hand pressure and drag forces resulting from the friction involved.

Lack of precise repeatability seems to be the major drawback to signature dynamics. In a field test conducted at the IBM Thomas J. Watson Research Center, this type of equipment exhibited a type I error rate of 1.7 percent and a type II error rate ranging from .02 percent for casual imposters to .4 percent in deliberate forgery attempts.

4. Speech Verification

Speech may be viewed as being made up of a series of transitions separated by regions of varying duration in which the sounds are relatively steady (Weinstein, 1975). The resulting harmonic structure is partly controllable and partly inherent to the individual. For verification purposes, devices quite often analyze the "steady" region. The user establishes a reference pattern by repeating a "training set" of selected utterances a number of times. The utterances are digitized and stored in the software system. The software system then segments the utterances, i.e., places emphasis on phenomena that are similar among

individuals. It then extracts those features which distinguish an individual from another. When verification is requested, it is those features which are compared. Examples of such features include time intervals between segmentation points, such as "v" and "b" in the utterance "available". Another distinguishable feature measures the pitch frequency between segmentation points (Dixon and Martin, 1979).

Type I and type II error rates have shown to be 1.1 and 3.3 percent respectively (Foodman, 1977). The average verification time is approximately 6.2 seconds. At present, speech verification is so expensive as to be cost prohibitive in the commercial marketplace.

5. Retinal Pattern Recognition

Retinal pattern recognition systems utilize the retina as a unique identifier(James, 1973; FIPS Pub 48, 1977, Pub 83, 1980). The blood vessels in the back of the eye form a pattern which has proven to be substantially different from individual to individual. Systems keying on this personal attribute take the retinal pattern and store it in memory for use as a reference. When an individual requests access, his/her retinal pattern is compared with that in memory. If the two blood vessel patterns match within a certain tolerance, admission is granted. Otherwise access is denied.

Use of retinal patterns as a personal attribute for verification purposes is the basis of this thesis. The device tested in this experiment is the Eye Dentify 7.5 System by Eye Dentify Inc. of Portland, Oregon. Description and function of this equipment is discussed in the following chapter.

III. DESCRIPTION OF THE EXPERIMENT

A. EQUIPMENT USED

The Eye Dentify 7.5 system is a biometric recognition access device utilizing the retinal pattern as the unique identifier. The premise is derived from studies showing with a high degreee of certainty that no two retinal formations are identical (Simon and Goldstein,1935,pp.901-906). This was further supported by Dr. Paul Tower(1955) whose study concluded that the greatest dissimilarity between identical twins occured in the blood vessel configuration of the retina.

In general, this system operates by storing reference information of the retinal pattern in a microprocessor and, upon entry demand, compares the stored information with the pattern of the individual seeking access at that time. If the stored information and that presented by the individual agree within limits, admittance is allowed.

If the data does not compare well, access is denied.

There are essentially two ways in which entry demand comparison takes place. The recognition mode requires no input of claimed identity from the individual seeking access. The live retinal pattern or "signature" is compared with each reference pattern stored in memory. When the verification mode is used, a personal identification number (PIN) must be entered prior to the "live" signature. It is then compared with that reference pattern in memory which is associated with that particular PIN.

The hardware components contained in the system include a binocular eyepiece, an electric camera, a microprocessor, printed circuit boards and subassemblies, a cast aluminum

housing with a 12-digit keypad, SCAN button, 8 character LED display, and power supply. Internal software stores eye signatures in memory, performs the matching process, controls system operations and allows I/O through 2 RS-232 ports for terminal and computer or printer interface. A system compatible display terminal is required to control system functions and operations.

The eye camera (ICAM) illuminates a fovea-centered circle on the back inside of the eye (including the retina and choroid) with an infrared emitting diode (IRED). This is the same infrared found in smoke detectors and television remote controls. The scanning spot centralized by the ICAM is 1.6 degrees in diameter and, as an external field half angle, is 10 degrees. See Figure 3.1 for the illustration of the scanning spot.

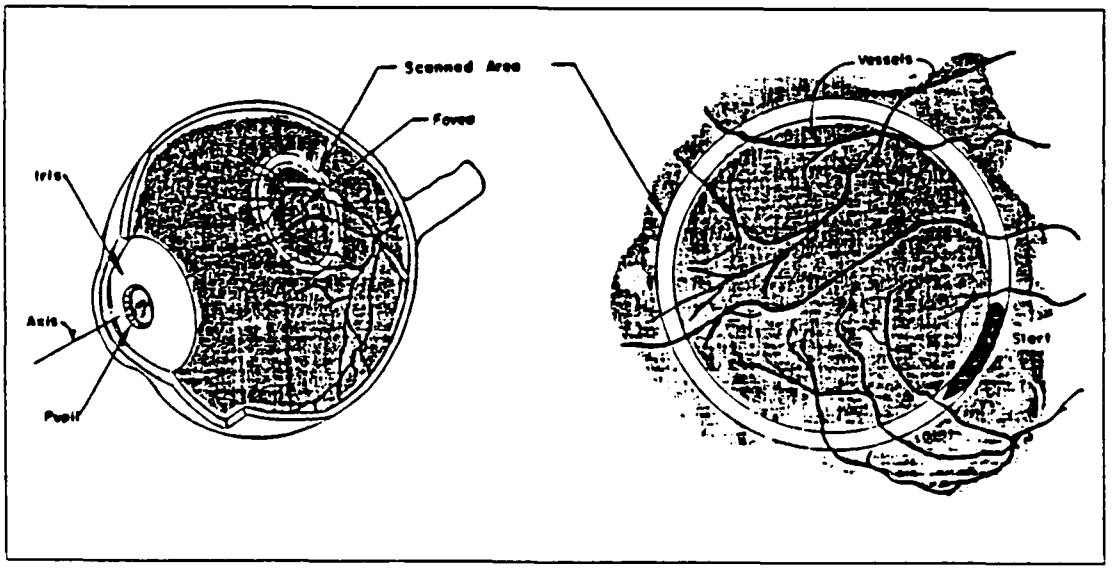


Figure 3.1 Scanning Spot, Extracted (Eye Dentify 7.5, 1984).

A total of 320 12-bit measurements are taken over a range of 450 degrees using an infrared wavelength centered

at 880 nanometers in the near-infrared region. Put simply, the ICAM makes 1.25 revolutions of the scanner and uses an infrared diode to illuminate and measure the light and dark areas of the retina and choroid in the scan circle. The resulting wavelength is then amplified, filtered, and converted from an analog to a digital signal. Head movements and slight variations in camera optics produce a low frequency modulation which are removed by a proprietary 4-step algorithm. This signal is then packed into 40 bytes(320 bits) called a template or signature. These templates are then either stored in memory or compared with what is in memory. Through enrollment the templates are stored in memory(IBANK) as reference templates. When access is requested, the template is converted into a time domain waveform. Subsequent live signatures from either the recognition or verification mode of operation are processed by a fourier cross correlation-based algorithm and matched to a reference waveform with respect to their phase and RMS amplitude. The two templates are then compared and a correlation score, expressed as a proportion, is generated. In addition, a software implemented phase corrector is used to compensate for eye rotation about the visual axis.

The identification threshold is that score above which the system decides there is sufficient correlation to assume that the live signature matches the reference template and below which the system decides there is a mismatch. When a match occurs access is granted. While the 7.5 system defaults to a threshold of .70 correlation, thresholds can be lowered to .60 or raised to .85 as desired.

In 1984 the Oregon Museum of Science and Industry in Portland, Oregon, conducted a study in which 2372 eye scans were acquired and stored on disc (Eye Dentify 7.5, 1984). 383 reference templates were stored into 7.5 memory and later transferred to a floppy disc. Each acquire was

compared with each reference template and a frequency distribution of correlation coefficients plotted. The results indicate that the probability of a type II error was 1E-06 at the .70 threshold, 1E-05 prob. at the .65 and 1E-04 at the .58 threshold when the phase corrector was in operation.

B. OBJECTIVE

The objective of this experiment was to determine the type I and type II error rate over a spectrum of correlation thresholds. The thresholds utilized represented the low, medium and high toleration levels allowed by the machine. In addition, observations would be made regarding the other measures of effectiveness so that conslusions could be drawn as to the acceptability of the 7.5 system as a computer security device. More specifically, it was anticipated that recommendations could be made as to the suitability of this system as a proper access control device in the military environment. If this device could prove to be reliable in terms of denying use to imposters while admitting authorized users, it could be applied to numerous systems in the military, especially in those areas where security is of paramount concern. It was with these objectives in mind that the experiment was conceived and completed.

C. EXPERIMENTAL PROCEDURE

Twenty-six subjects participated on a volunteer basis,twenty-four of which were military officers, both U.S. and international, between the ages of 25 and 35 who were assigned as students at the Naval Postgraduate School. None of the subjects were color blind or had, in any way, some form of opthomological disease for which they were under medical treatment. There was a good cross-section of

subjects whose vision was corrected through the use of glasses, or hard or soft contact lenses. None of the subjects were familiar with the 7.5 system in that they had never used it under operational conditions.

A standard system-compatible RS-232 display terminal was used to operate the menu driven internal software that controls the system's operation.

Step one of the experiment required each subject to enroll into the system. The enrollment process is the procedure by which the retinal pattern is converted into a template and stored in memory. This is the reference template against which all other signatures are compared when access is requested.

As each subject arrived to enroll, he was given the following instructions to increase the probability of building an accurate reference template:

1. Look into the binocular-type eyepiece
2. Fix your view on an object resembling a daisy wheel. This view is seen through the right eye only. The left eyepiece is for comfort only.
3. Shift your head until all or most of the red is eliminated from the daisy.
4. When the daisy appears green or white concentrate on the center of it and press the SCAN button located on the face of the machine.

Depression of the SCAN button activates the ICAM mechanism and a template is constructed. The enroller then chose one of the following options:

1. allow the enrollee to repeat the process which results in the construction of another template.
2. restart the process. When restart is activated only the previous scan is retained. All other templates not stored in memory are discarded with the previous template becoming the reference.

3. cancel the process. All templates not stored in memory are discarded and the entire enrollment process must be reinitiated.
4. finish the enrollment process.

Upon completion of a second SCAN or acquire, a numerical score is displayed to the enroller. This score ranges from -1.00 to +1.00 and represents the correlation between the reference template and the subsequent acquire. The enroller then chose to either accept or reject the latter signature. If the signature was accepted it was averaged with the reference template creating a new reference. A template that was rejected was simply discarded with no change made to the reference signature.

Each subject was guided through the same enrollment process. The goal was to average four templates to the reference to which each correlated with a score no lower than +.90. This at times required over twenty scans by some subjects. If scores were consistently below +.90, the restart was initiated as it was concluded that the reference template was poor. If, after restart, scores were still consistently below +.90 the cancel option was used and the enrollment process reinitiated. To Finish the enrollment, a user identification name and personal identification number (PIN) was assigned to the template and stored in memory. All subjects were enrolled into the 7.5 system prior to the next phase of the experiment.

As previously stated, the Eye Dentify 7.5 is capable of operating at thresholds specified by the system operator. Utilization of thresholds of +.60, +.72 and +.85 were expressly chosen for the design of this experiment. This represents the low medium and high ranges allowed by the system. Each subject attempted to gain access (be recognized) over each of the three thresholds. At each testing session a total of six trials were recorded for each

subject. A trial is the attempted access at one particular threshold by a subject. After each trial the threshold level was changed. The order of threshold testing was randomly assigned to each subject. When a trial at each threshold was completed the process was executed a second time and the session ended.

A subject was required to wait at least one hour between sessions. This, as well as the order of threshold testing, was embedded into the experimental design to negate the possible effects associated with the learning curve known to be related to the 7.5 system. As the subject becomes more familiar with the equipment, the better he is able to focus on the daisy and properly align his eye with the ICAM. This results in a more accurate scan.

The recognition mode was used throughout the experiment. Subjects were not required to do more than request access by focusing their view on the daisy wheel and activating the scan mechanism. If the verify mode were used the subject would have been required to input their pin before the scan process. A printer was connected to the 7.5 system which would simulate the use of a security log and record the results of each access attempt. For any one trial a subject who was not recognized would be instructed by the system to repeat the attempt and "not recognized" would be annotated on the printout. Three consecutive non-recognitions by one subject resulted in the subject being instructed to "see security" and similar output was displayed on the printer. Subjects receiving three consecutive non recognitions were considered to have been denied access for that particular trial.

A record was kept which documented the subject, trial number, and threshold during each session. Annotations were made indicating whether a subject was recognized on the first , second, or third attempt, or whether he was denied access.

D. RESULTS

The data collected on the recognition rate of the 7.5 system were expected to be binomial in nature (Winer, 1971). In order to stabilize the variances, the data was transformed using the arcsin transformation, $y' = 2\arcsin\sqrt{y}$. A level of significance, α, of .05 was selected during the design phase.

Records of observations were tabulated, specifying for each subject the percentage of recognitions out of a possible twelve at each threshold. The recognition rate for all subjects at each threshold are shown in Table I.

A two way factorial analysis of variance was performed on the transformed data. The Results are summarized in Table II. The analysis showed the effect of threshold levels to be significant ($F = 39.02$, $df = 2/50$, $p < .0005$). A range test on means (Hicks, 1973) was performed to determine which threshold levels were significantly different. It was concluded that at the $\alpha = .05$ level there were significant differences between the .60 and .85 thresholds and between the .72 and .85 thresholds. No significant difference was found between the .60 and the .72 levels.

Figure 3.2 shows the overall recognition rates over all three thresholds. As can readily be seen, there is a marked decrease in recognitions from the .60 level(95%) to the .85 level(69%).

TABLE I

RECOGNITION RATES

.60 Correlation Threshold	
1st Attempt	84%
2nd Attempt	9%
3rd Attempt	2%
Not Recognized	5%

.72 Correlation Threshold	
1st Attempt	72%
2nd Attempt	16%
3rd Attempt	4%
Not Recognized	8%

.85 Correlation Threshold	
1st Attempt	40%
2nd Attempt	19%
3rd Attempt	10%
Not Recognized	31%

Overall	
.60	95%
.72	92%
.85	69%

TABLE II

ANALYSIS OF VARIANCE FOR THE 7.5 SYSTEM RECOGNITION RATE

SOURCE	DF	SS	MS	F	Significance
Subjects	25	16.617	0.665	.132	**
Threshold	2	10.066	5.033	39.020	**
Error	50	06.425	0.129		
Total	77	33.108			

** P < .0005

Figure 3.3 plots the recognition rate for each attempt over the three thresholds. For the trials as a whole, at the .60 level, 84% were recognized on the first attempt, 9% were recognized on the second attempt, 2% on the third attempt and 5% were not recognized at all. Yet as Figure 3.4 illustrates, at the .60 threshold, 55% of those remaining(16%) who were not recognized on the first attempt were recognized on the second; of the 7% remaining subjects who were not recognized on either the first or second attempt, 33% were admitted on the 3rd attempt. When subjects were not recognized on the first attempt, 31% of those remaining were not recognized at all at the .60 level, 28% at the .72, and 53% were not recognized at the 85% threshold (see Figure 3.5).

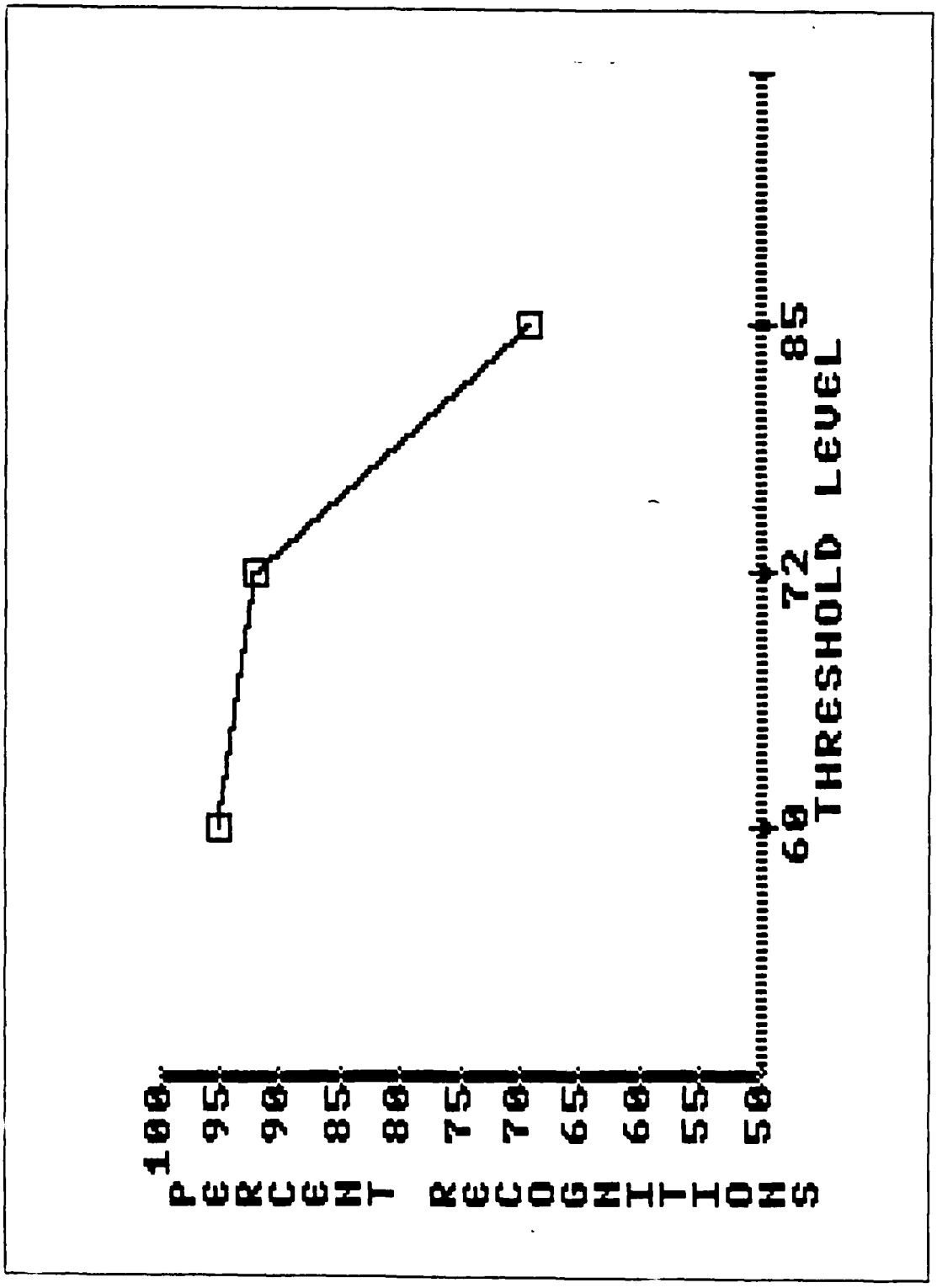


Figure 3.2 Overall Recognition Rate.

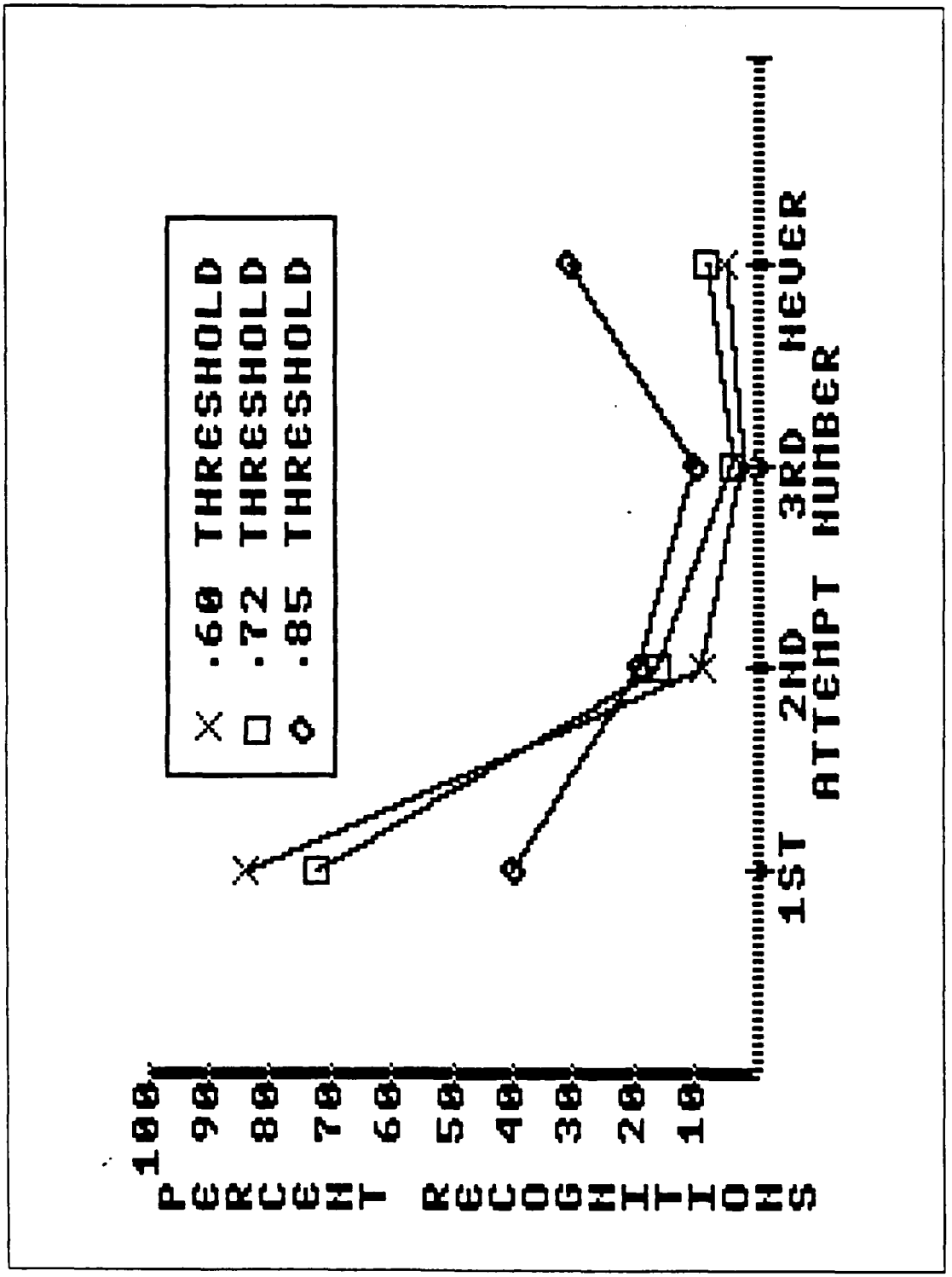


Figure 3.3 Recognition Pattern.

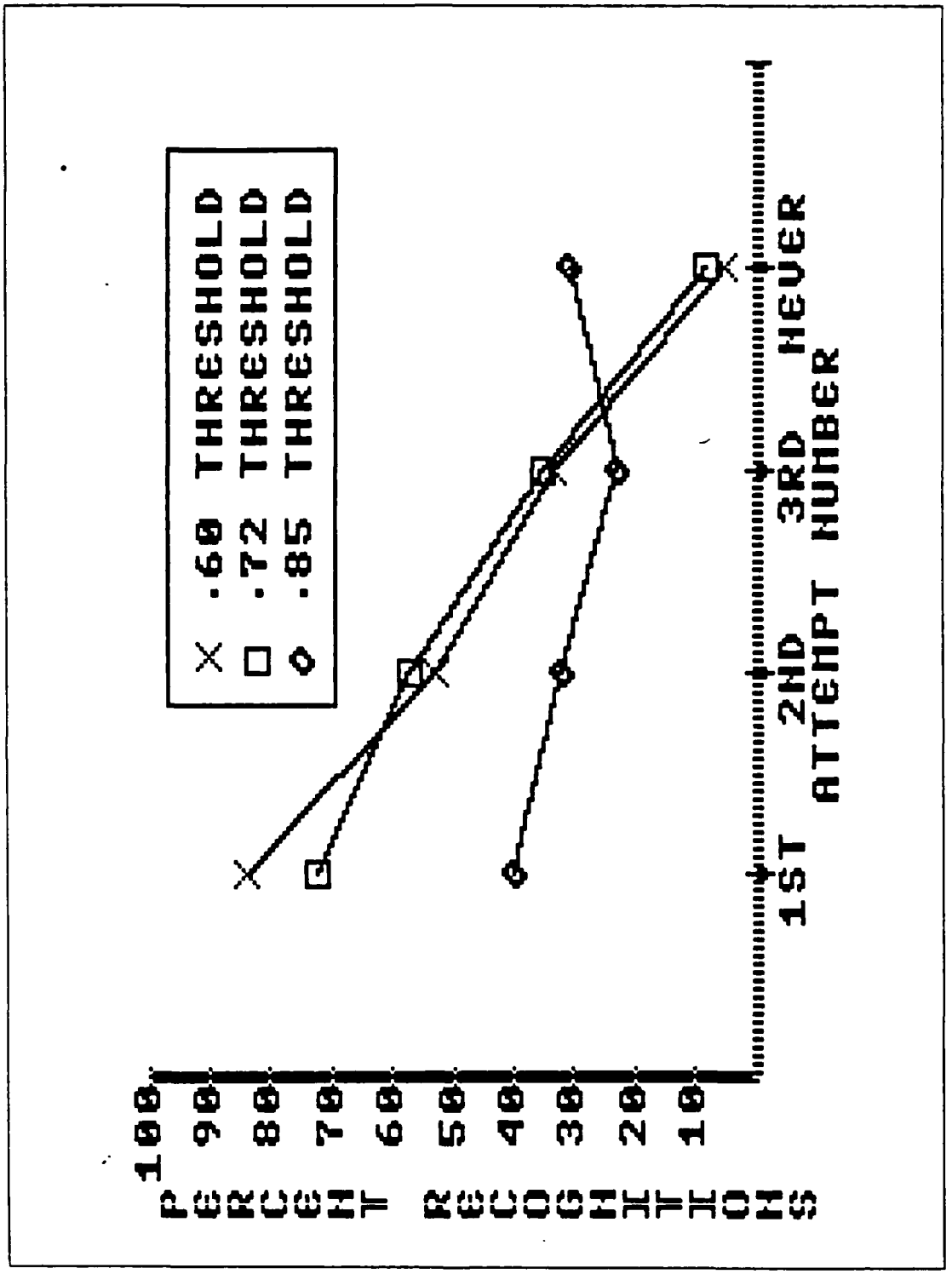


Figure 3.4 Recognition Rate, Remaining Attempts.

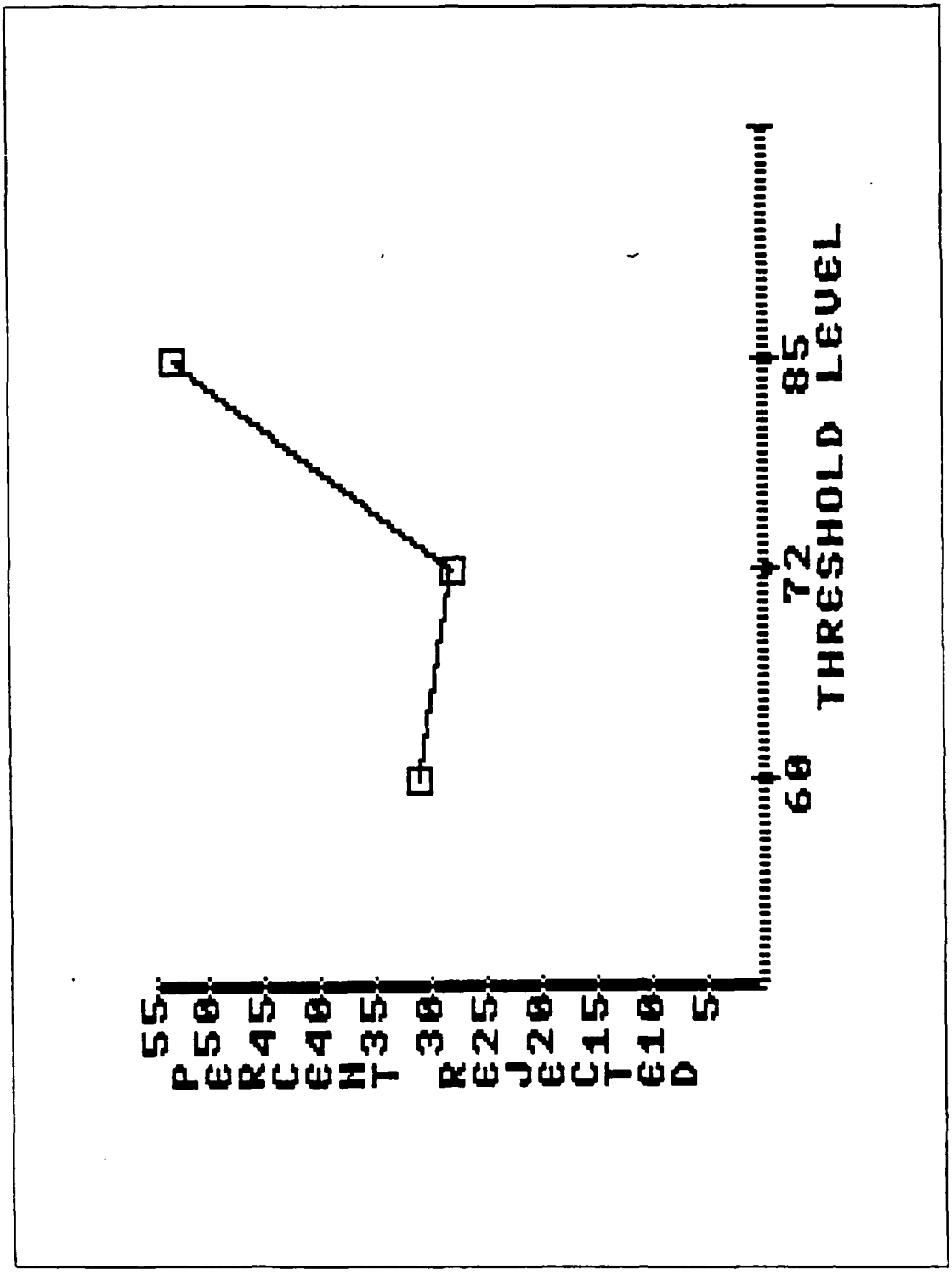


Figure 3.5 Non-Recognition Rate, Remaining After 1st Attempt.

IV. DISCUSSION AND CONCLUSIONS

A. DISCUSSIONS

1. Type I and Type II Error Rate

As previously suggested in the discussion about the recognition rates, type I error rates were found to be 5% at .60, 8% at .72 and 31% at the .85 correlation threshold. In the approximately 6,000-7,000 scans that were taken, in a pilot experiment, practice and during the actual experiment, there were zero misrecognitions (see Table III).

TABLE III
TYPE II ERROR RATES

THERE WERE NO
TYPE II ERRORS
IN THIS EXPERIMENT

Evidence from this experiment indicates there is no reason to suggest that the calculations for the probability for type II errors determined by the Oregon study are incorrect. Eye Dentify, Inc. advertised a 1% type I error rate yet no formal experiment was published which indicates that this probability was tested.

One factor which seems to have had a significant impact on the type I error rate was the enrollment process. During enrollment, one of the subjects was unable to achieve the goal which, as previously stated, was to average four templates with the reference, each with a correlation score no lower than +.90. After numerous scans the subject could only achieve two scores which correlated high enough to be averaged with the reference. Subsequently, she had difficulty being recognized by the system. When her experiment data is ignored, the overall type I error rate drops to 2% at .60, 5% at .72 and 29% at .85 correlation. In addition, when this subject was re-enrolled at the conclusion of the experiment, five "good" templates were achieved and averaged. She then attempted to gain access and was consistently recognized by the 7.5 system at all three thresholds.

The results of a pilot experiment further support this theory. In the pilot test, subjects were enrolled by averaging the first five scans with the reference template regardless of their correlation scores. As a result, type I errors were significantly higher (16% at .60, 26% at .72 and 49% at .85). Figure 4.1 illustrates the comparison of the pilot test data with the experimental data after adjustment for the poor enrollee. As can be seen, the pilot test scores are 84% recognized at the .60 threshold, 74% at .72 and only 51% were recognized at the .85 correlation level.

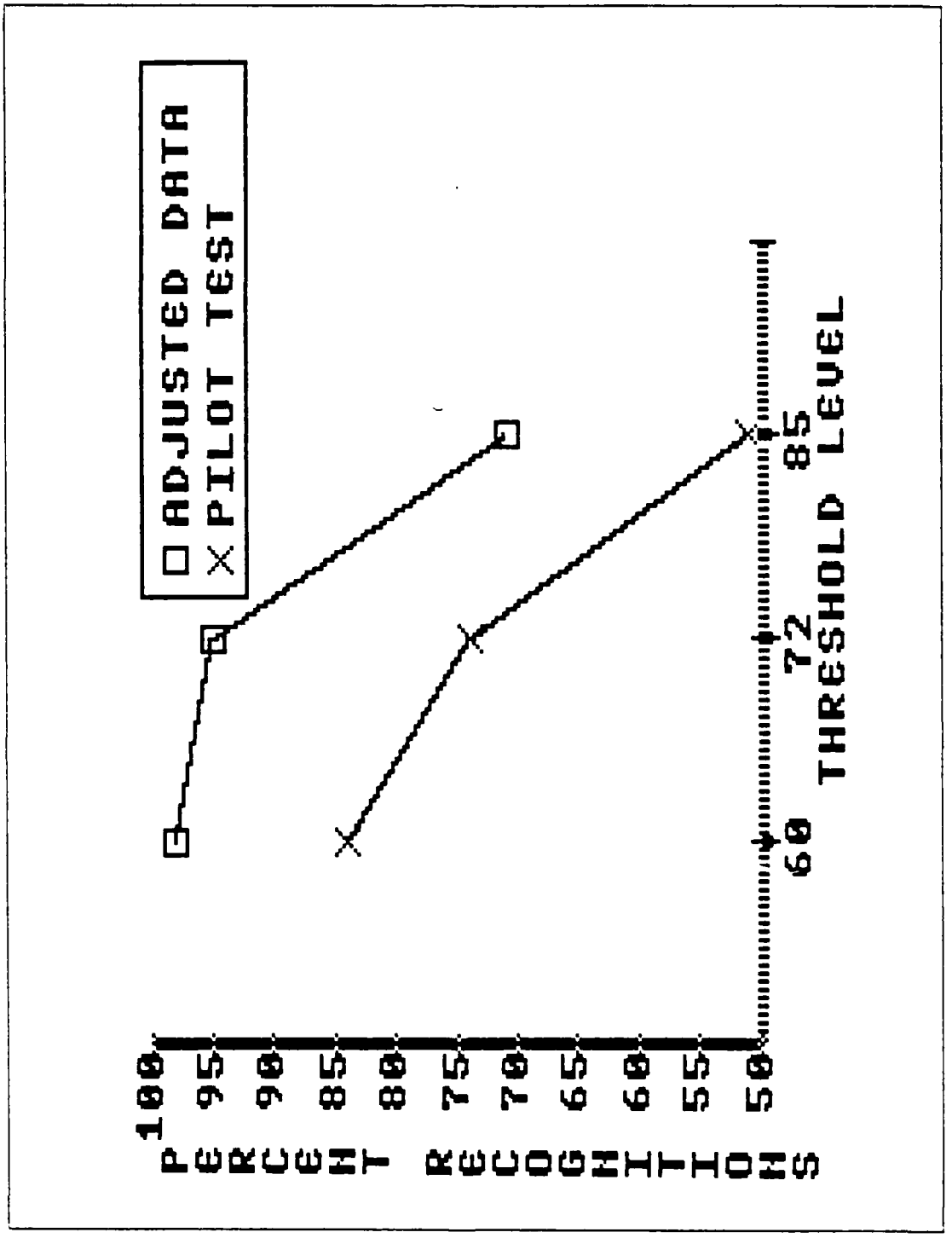


Figure 4.1 Pilot Test Results vs Adjusted Experimental Data.

Another noteworthy observation deals with the use of contacts or glasses. Neither had any effect on the recognition rate of the system. Those with glasses were instructed to remove them prior to enrollment or access request. Those wearing soft or hard contact lens attempted to gain access without them at various times throughout the experiment. No difference in recognition ability was noticed.

2. Other Measures of Effectiveness

a. Susceptibility to Circumvention

As previously stated, the microprocessor and subassemblies are located in a cast aluminum housing. Access to the processor and printed circuit boards is through the back of the machine via a key lock. If it is mounted onto a wall, all connecting wires would be through the wall. Anyone attempting to bypass or intercept transmissions would have to dismount the device.

b. Time to Achieve Recognition

This experiment was not designed to precisely estimate the time to recognition. However, through observations it was estimated that it took 2-3 seconds from the time the scan button was activated to acceptance and 5-7 seconds if rejected by the system. Added to this must be the time it took to fixate on the daisy wheel as well as the time for each subsequent attempt before recognition.

c. Convenience to the User

This system is very easy to use in many ways. When the recognition mode is used, the individual need not remember any passwords or numbers. Learning to use the device is quite simple. All the individual needs to do is

concentrate on a fixation point and activate the SCAN button. Sometimes, however, it is difficult to focus properly on this point. Frustration increasingly becomes a factor when additional attempts are necessary. It was observed through the experiment that the enrollment process proved to be more time consuming and frustrating than had been anticipated. Of the 32 subjects who were enrolled, 24 required 10 or more SCANS to acquire five templates correlating +.90 or better with the reference. 11 of those 24 required in excess of 20 SCANS to accomplish that goal.

d. Computer System Processing Requirements

The Eye Dentify 7.5 System is designed primarily as a physical access device only. Additional software is available (purchased separately) which makes interface with a computer system possible. However, in order for this system to be used for access to systems and applications programs, additional software must be written. This would require processing capability and storage at the central facility as the microprocessor is incapable of doing this. In addition, if the system were to be used at a large facility which has more than 1200 individuals requiring access, additional space would be needed from the central computer to store those reference templates.

e. Reliability and Maintainability

The 7.5 system performs consistently and is fairly maintenance-free. The software has proven reliable and hardware components such as printed circuit boards and subassemblies can be easily replaced when failure occurs.

f. Cost of the System

The purchase price of this retina scan device is $10K. The proms required for computer system interface cost

approximately $500. The amount of money that would be required to develop the software to support this interface would depend on its applications. The applications programs would be unique to the system utilized and a price cannot be quoted without a feasibility study. Nevertheless, these costs must be considered when determining the cost of the system.

B. CONCLUSIONS

The Eye Dentify 7.5 system is a fairly expensive, highly reliable access control device. Its probability for false recognitions is far better than most other known devices. It can be used as a physical access device at virtually any military installation where access devices are used. The larger the installation, the more consideration must be given to its time to recognition. If a large queue forms for those awaiting admission, methods may be invented by authorized users to circumvent the system altogether, thereby negating the purpose of the system. The best applications for this in the military environment seems to be at small installations where time is not a significant factor yet denial of access to unauthorized users is vital to security.

As a device for access to computer systems and applications programs, the 7.5 system is not yet ready to replace passwords. The price of the equipment plus the expense necessary for the development of associated software make it cost prohibitive for most computer systems. Final determination, however, lies in the hands of the potential buyer. For some systems this may be a small price to pay for the assurance of a one in a million chance for intrusion by a would be perpetrator. The information to be protected may be so sensitive that management is willing to pay the

costs as well as endure the frustration of authorized users who encounter false rejections (type II errors).

C. FURTHER RESEARCH RECOMMENDATIONS

The Eye Dentify 7.5 system is still relatively new to the marketplace. Very little research regarding this system has been published. The following represents just some of the areas in which this system could be tested.

1. Test the effect of enrollment upon type I error rates. When authorized users are consistantly rejected, can re-enrollment reduce the error rate?
2. Test this equipment on a moving platform Is it feasible to apply this access control device to shipboard applications?
3. Develop the necessary software and test the possible applications when interfacing with a central host or distributed computer system.
4. What effects do different lighting conditions have on the reliability of the system?
5. What are the type I and type II error rates when two eyes are used as a reference rather than one eye?
6. What are the effects of electromagnetic pulse on the system?
7. Design an experiment to accurately determine the average time to recognition for the 7.5 device.
8. What are the type I and type II error rates for the 7.5 system when the verification mode is used instead of the recognition mode? (Maxwell)
9. What happens to the system when the number of reference templates in memory approaches or exceeds 1200?
10. Conduct this same experiment over a wide range of age groups. Does age affect the performance of this system?

LIST OF REFERENCES

Dixon, N. and Martin, T., Automatic Speech and Speaker Recognition, The Institute of Electrical And Electronic Engineers, Inc., NY,NY 1979.

DOD Computer Security Center, "Computer Security, the Defense Department and the Private Sector - Part III - DOD Computer Center's Response", Computer Security Journal, Summer 1984.

Epperly, E., Survey of Federal Computer Security Policies, Office of the Secretary of Defense. Washington, D.C., November, 1980.

Eye Dentify Inc., 7.5 Camera Function Definition, unpublished, 1984.

Fauer, L. and Courtney, R., "Computer Security, the Defense Department, and the Private Sector - A 3 Part Dialogue About Fundemental Objectives and Needs", Computer Security Journal, Summer 1984.

Fejfar, A., Test Results - Advanced Delvelopment Models of BISS Identity Verification Equipment, Vol. IV, Automatic Fingerprint Verification, MTR-3442, Vol. III, the Mitre Corporation, Bedford, Ma., September, 1977.

FIPS, Federal Information Processing Standards Publication 48, Guidelines on Evaluation of Techniques for Automated Personal Identification, U.S. Department of Commerce, National Bureau of Standards, April, 1977.

FIPS, Federal Information Processing Standards Publication 83, Guidelines on User Authentication Techniques for computer Network Control, U.S. Department of Commerce, National Bureau of Standards, September, 1980.

Foodman, M., Test Results - Advanced Development Models of BISS Identity Verification Equipment, Vol. II, Automatic Speaker Verification, MTR-3442, Vol. II, The Mitre Corporation, Bedford Ma., September, 1977.

Hicks, C., Fundemental Concepts in the Design of Experiments, Holt, Rinehart and Winston, NY NY, 1973.

Hoffman, L., Modern Methods for Computer Security and Privacy, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1977.

James, M., Security, Accuracy, and Privacy in Computer Systems, Prentice-Hall, Inc., Englewood Cliffs, NJ., 1973.

Landwehr, C., "The Best Available Technologies for Computer Security", Computer, July, 1983.

Landwehr, C., A Survey of Formal Models for Computer Security, Naval Research Laboratory, Washington, D.C., 30 September 1981.

Maxwell, R., The Status of Personnel Identity Verifiers Sandia National Laboratories, Albuquerque, NM, unpublished, undated.

National Bureau of Standards, Proceedings of the Computer Security Initiative Program, Gaithersburg, Md., July 17-18, 1979.

Peterson, J., and Silberochotz, A., Operating System Concepts, Addison-Wesley Publishing, Inc., Reading, Ma., 1984.

Simon, C. and Goldstein, I., New York State Journal of Medicine, Vol. 35, September 15, 1935, no. 18, pp 901-906.

Tangney, J., History of Protection in Computer Systems (Technical report), MTR-3999, Mitre Corporation, Bedford, Ma., July, 1980.

Tower, P. The Fundemental Oculi in Monozygotic Twins, American Medical Association Archives of Opthamology, Vol. 54, 1955, pp. 225-238.

Ware, W., Security, Privacy and New Technology, Rand Corporation, Santa Monica, Ca., January, 1981.

Weinstein, C., McCandless, S., Mondshein, L., and Zue, V., A System fro Acoustic-Phonetic Analysis of Continuous Speech, Automatic Speech and Speaker Recognition, N. R. Dixon and Thomas B. Martin, Editors, IEEE Press, Piscataway, NJ, 1979, pp. 312-327.

Winer, B., Statistical Principles in Experimental Design, McGraw-Hill Book Co., NY NY, 1971.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey California 93943-5100	2
3.	Computer Technology Programs, Code 37 Naval Postgraduate School Monterey California 93943-5100	1
4.	Professor Gary K. Poock Code 55PK Department of Operations Research Naval Postgraduate School Monterey California 93943-5100	35
5.	Professor Jack LaPatra Code 54LP Department of Administrative Sciences Naval Postgraduate School Monterey California 93943-5100	1
6.	Assistant Professor Doug Neil Code 55NI Department of Operations Research Naval Postgraduate School Monterey California 93943-5100	1
7.	LT Debra K. Helle IS Support Division NMPC 47 Department of the Navy Washington D.C. 20350	3
8.	John O'Hare, Code 442EP Office of Naval Research 800 North Quincy Street Arlington Virginia 22217	1
9.	Jesse Orlansky Institute for Defense Analysis Science and Technology Division 1801 North Beauregard Street Alexandria Virginia 22311	1
10.	Jerry Malechi Code 442EP Office of Naval Research 800 North Quincy Street Arlington Virginia 22217	1
11.	Russell Maxwell Systems Engineering Division 5264 Sandia National Laboratories Alburquerque New Mexico 87185	1

12. Bob Sasmore 1
Director of Basic Research
Army Research Institute
5001 Eisenhower Avenue
Alexandria Virginia 22333

13. CAPT Paul Chetelier 1
OUSD R&D
Room 3D129 Pentagon
Washington D.C. 20301

14. Dave Pallett 1
National Bureau of Standards
Building A216
Gathersburg Maryland 20899

15. Don McKechnie 1
AFAMRL/HEF
Wright Patterson AFB Ohio 45433

16. Dale Nelson 1
Eye Dentify Inc.
Box 3827
Portland Oregon 97208

17. Bob and Beverly Williges 1
Department of IE & OR
Virginia Polytechnical Institute
130 Whittmore Hall
Blacksburg Virginia 24061

18. CDR Tyce DeYoung 1
SPAWARSYSCOM, Code 6131
Washington D.C. 20363-5100

19. Chuck Fargo 1
7842 Melba Avenue
Canoga Park California 91404

20. Dick Chanda 1
Rockwell International
Rocky Flats Plant
Box 464
Golden Colorodo 80401

21. Richard Freeman 1
Gordian Systems
3512 West Bayshore Road
Palo Alto California 94303

22. Dohn Pagel 1
630 Price Avenue
Redwood City California 94063

END

FILMED

12-85

DTIC